AU/ACSC/028/2001-04

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

AIR FORCE INFORMATION OPERATIONS (IO) DOCTRINE: CONSISTENT WITH JOINT IO DOCTRINE?

by

Robert E. Blackington, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Lieutenant Colonel James M. Jenkins

Maxwell Air Force Base, Alabama

April 2001

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	4/1/2001	Report 4/1/2001

4. TITLE AND SUBTITLE
Air Force Information Operations (IO) Doctrine: Consisten with Joint IO Doctrine?

5. FUNDING NUMBERS

6. AUTHOR(S)
Blackington, Robert E.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Command and Staff College Air University

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

Is Air Force information operations (IO) doctrine consistent with joint IO doctrine as required by policy directives? To answer this question, this research paper analyzes the consistency between Air Force Doctrine Document (AFDD) 2-5, Information Operations, and Joint Pub (JP) 3-13, Joint Doctrine for Information Operations, in three principal areas:
1. The components of information superiority (IS) and definitions of the key terms IS, IO, and information warfare (IW).
2. Air Force addition of the terms counterinformation (CI), offensive counterinformation (OCI), and defensive counterinformation (DCI). 3. The capabilities and related activities used to carry out offensive and defensive IO.
The author concludes that AFDD 2-5 is inconsistent with JP 3-13 and offers two alternative doctrinal constructs to correct this deficiency. Having concluded that Air Force and joint

14. SUBJECT TERMS
IATAC Collection, information operations, Air Force

15. NUMBER OF PAGES
60

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

DISCLAIMER ii

ILLUSTRATIONS IV

TABLES V

PREFACE VI

ABSTRACT VII

INTRODUCTION 1

BACKGROUND 3
The Significance of Joint Doctrine 3
The Significance of Service Doctrine 5
The Relationship between Air Force and Joint Doctrine 7
AFDD 2-5 and JP 3-13 7

ISSUE ANALYSIS 9
The Components of Information Superiority and Key Definitions 9
Air Force Addition of the Terms Counterinformation (CI), Offensive Counterinformation (OCI), and Defensive Counterinformation (DCI) 17
Capabilities and Related Activities 19
Is AFDD 2-5 Consistent with JP 3-13? 25
Strategic, Operational, and/or Tactical Level Impact 26

SUMMARY/CONCLUSIONS/RECOMMENDATIONS 32

POTENTIAL IMPACT FROM DOCTRINAL DIFFERENCES 39

BIBLIOGRAPHY 52

Illustrations

Page

Figure 1. Joint Information Superiority Construct.....10

Figure 2. Air Force Information Superiority Construct.....11

Figure 3. Air Force Information Superiority Construct--Alternative #1 35

Figure 4. Air Force Information Superiority Construct--Alternative #2 36

Tables

Page

Table 1. Key Definitions.....15

Table 2. Offensive IO, Defensive IO, OCI and DCI Definitions 18

Table 3 Potential Impact from Doctrinal Differences.....40

Preface

Since Operation DESERT STORM, there is arguably no other topic within the Department of Defense (DOD) that has received more attention, or generated more controversy, than information operations (IO). In the wake of that conflict, numerous magazine articles, books, and papers were published on the subject as the DOD struggled to define this new phenomenon. In 1995, both the Joint Staff and Services consolidated their ideas as the first drafts of joint and Service doctrine circulated around the DOD. What these early efforts illustrated was that there was no clearly settled consensus on IO. Following the Army's lead, the Air Force finalized and published its IO doctrine in August of 1998, while the Joint Staff published its doctrine in October of that same year. The fact that joint doctrine was published after Air Force doctrine is significant.

Joint Chiefs of Staff Pub 2 establishes the relationship between Service and joint doctrine. It states that each Service will ensure that its doctrine and procedures are consistent with joint doctrine established by the Chairman of the Joint Chiefs of Staff. Since Air Force IO doctrine was finalized before joint IO doctrine, this raises a fundamental question: is Air Force IO doctrine consistent with joint IO doctrine? The purpose of this research paper is to answer that question. If Air Force IO doctrine is found to be inconsistent with joint doctrine, this paper will then explore whether there has been any negative impact to military operations at the strategic, operational, and/or tactical levels due to the inconsistency.

Abstract

Is Air Force information operations (IO) doctrine consistent with joint IO doctrine as required by policy directives? To answer this question, this research paper analyzes the consistency between Air Force Doctrine Document (AFDD) 2-5, Information Operations, and Joint Pub (JP) 3-13, Joint Doctrine for Information Operations, in three principal areas:

1. The components of information superiority (IS) and definitions of the key terms IS, IO, and information warfare (IW).

2. Air Force addition of the terms counterinformation (CI), offensive counterinformation (OCI), and defensive counterinformation (DCI).

3. The capabilities and related activities used to carry out offensive and defensive IO.

The author concludes that AFDD 2-5 is inconsistent with JP 3-13 and offers two alternative doctrinal constructs to correct this deficiency.

Having concluded that Air Force and joint IO doctrine are inconsistent, the author explores whether there has been any negative impact to military operations at the strategic, operational, and/or tactical levels due to the inconsistency. To answer this question, the author looks at Operation ALLIED FORCE. Research of unclassified sources reveals that the absence of public affairs (PA) as an offensive or defensive activity in Air Force IO doctrine caused significant problems. The potential impact of other doctrinal inconsistencies on future operations is highlighted in Appendix A.

Chapter 1

Introduction

At the very heart of war lies doctrine. It represents the central beliefs for waging war in order to achieve victory...It is the building material for strategy. It is fundamental to sound judgement.

—General Curtis E. LeMay, USAF

When our nation calls on the military to achieve its objectives, Service forces must seamlessly integrate into an efficient and effective joint fighting team. A body of joint doctrine, embracing fundamental principles forged from our warfighting heritage, must be the guide and common frame of reference for joint force action. As Joint Pub (JP) 1-01.1, Compendium of Joint Publications, states, "A workable and effective joint doctrine may well constitute the difference between ensuring the well-being of those sent into combat, or risking their loss because of the employment of procedures and tactics which do not optimize the coordinated capabilities of all the Services."[1] To capitalize on the synergistic effect achieved by joint force employment, Service forces must be well-versed not only in joint doctrine, but in their own doctrine as well. Like joint doctrine, Service doctrine provides guidance and a common frame of reference to prepare and employ Service forces. In other words, Service doctrine shapes how the Service will organize, equip, and train for joint employment. For this reason, Service doctrine must be consistent with joint doctrine. In fact, this is Joint Chiefs of Staff policy. According to Joint Chiefs of Staff (JCS) Pub 2, "Each Service will ensure that its doctrine and procedures are Consistent [sic] with joint doctrine established by the Chairman of the Joint Chiefs of Staff."[2]

Although joint doctrine doesn't establish policy, there are four exceptions: JP 0-2, Unified Action Armed Forces (UNAAF); JP 1, Joint Warfare of the Armed Forces; JP 1-01, Joint Doctrine Development System; and JP 1-01.1, Compendium of Joint Publications.[3] Three of these publications, JP 1, JP 1-01, and JP 1-01.1, also state that Service doctrine must be consistent with approved joint doctrine. [4] Based on this policy guidance, it would seem logical that the Services would wait for joint doctrine to be finalized before publishing their own doctrine. For Air Force IO doctrine, this wasn't the case. Between 1995 and 1998, Air Force IO doctrine and joint IO doctrine were developed concurrently, with Air Force Doctrine Document (AFDD) 2-5, Information Operations, actually predating JP 3-13, Joint Doctrine for Information Operations, by more than 2 months. This raises a fundamental question. Is Air Force IO doctrine consistent with joint IO doctrine? If AFDD 2-5 is found to be inconsistent with JP 3-13, there could be negative impacts to military operations at the strategic, operational, and/or tactical levels due to the inconsistency. To find out if Air Force IO doctrine is consistent with joint IO doctrine, this research paper will analyze consistency in three principal areas:

1. The components of information superiority (IS) and definitions of the key terms IS, IO, and information warfare (IW).

2. Air Force addition of the terms counterinformation (CI), offensive counterinformation (OCI), and defensive counterinformation (DCI).

3. The capabilities and related activities used to carry out offensive and defensive IO.

Notes

[1] Joint Pub (JP) 1-01.1, *Compendium of Joint Publications*, 23 April 1999, A-5.
[2] Ibid., Figure A-1, A-2.
[3] JP 1-01, *Joint Doctrine Development System*, 5 July 2000, I-1.
[4] JP 1, *Joint Warfare of the Armed Forces of the United States*, 10 January 1995, I-4; JP 1-01, *Joint Doctrine Development System*, 5 July 2000, I-2; and JP 1-01.1, *Compendium of Joint Publications*, 23 April 1999, A-2.

Chapter 2

Background

> *Doctrine provides a military organization with a common philosophy, a common language, a common purpose, and a unity of effort.*
>
> —General George H. Decker, USA

Before we analyze the consistency between AFDD 2-5 and JP 3-13, we need to answer three basic questions. First, what is the significance of joint doctrine? Second, what is the significance of Service doctrine? And finally, what is the relationship between Service and joint doctrine? We'll conclude this chapter with a brief look at the development and relationship between AFDD 2-5 and JP 3-13.

The Significance of Joint Doctrine

For the uninitiated, the role or purpose of joint doctrine can be confusing. Is it policy, strategy, or merely guidance for our Armed Forces? According to JP 1-01, Joint Doctrine Development System:

> The purpose of joint doctrine...is to enhance the operational effectiveness of US forces. With the exception of JP 1, *Joint Warfare of the Armed Forces of the United States*, JP 0-2, *Unified Action Armed Forces (UNAAF)*, JP 1-01.1, *Compendium of Joint Publications*, and this publication, joint doctrine...will not establish policy. Joint policy will be reflected in Chairman of the Joint Chiefs of Staff (CJCS) Instructions (CJCSIs) or CJCS Manuals (CJCSMs). These instructions and manuals are not joint publications, but contain CJCS policy and guidance that does not involve the employment of forces.[1]

To further clarify the purpose of joint doctrine, JP 1, Joint Warfare of the Armed Forces of the United States, claims, "Though neither policy nor strategy, joint doctrine deals with the fundamental issue of how best to employ the national military power to achieve strategic ends."[2] Finally, JP 1-01 offers additional insight by defining joint doctrine as:

> Fundamental principles that guide the employment of forces of two or more Military Departments in coordinated action toward a common objective. Joint doctrine is authoritative; as such, it will be followed except when, in the judgement of the commander, exceptional circumstances dictate otherwise. It will be promulgated by, or for, the Chairman of the Joint Chiefs of Staff, in coordination with the combatant commands and Services.[3]

In sum, joint doctrine is neither policy (except for those publications cited above) nor strategy, but it does provide authoritative guidance for the employment of the Armed Forces. Now that we've established the purpose of joint doctrine, let's expound on its significance. To frame our discussion, we'll focus specifically on the policy documents JP 1, JP 1-01, and JP 1-01.1.

When discussing the significance of joint doctrine, two recurring themes prevail. First, joint doctrine embodies lessons learned from past training, exercises, and operations. And second, these lessons form the foundation for thinking about, planning, and executing future joint operations. Joint Pub 1 embraces these ideas. When discussing lessons learned, JP 1 states that "Military doctrine presents fundamental principles that guide the employment of forces...It provides the distilled insights and wisdom gained from our collective experience with warfare."[4] The publication goes on to state that these principles, insights, and wisdom "offer a common perspective from which to plan and operate, and fundamentally shape the way we think about and train for war; facilitate clear thinking and assist a commander in determining the proper course of action; and deal with the fundamental issue of how best to employ the national military power to achieve strategic ends."[5] Joint Pub 1-01 echoes these same themes.

Like JP 1, JP 1-01 discusses how joint doctrine embodies lessons learned from the past and then uses them as a foundation to guide and enhance joint force employment. Joint Pub 1-01 defines joint doctrine as "Fundamental principles that guide the employment of forces of two or more Military Departments in coordinated action toward a common objective."[6] These principles are also used to "enhance the operational effectiveness of US forces."[7] Joint Pub 1-01.1 also reiterates these themes.

When creating joint doctrine, JP 1-01.1 claims that training, exercises, past operations and "Every possible contingency where the US military could be involved is being examined to ensure that sound doctrine and procedures exist."[8] This doctrine is designed to "improve both interoperability and efficiency, improve the combat effectiveness of the US military forces, and focus unity of effort."[9]

The significance of joint doctrine can best be summed up by the quote appearing in the introduction, "A workable and effective joint doctrine may well constitute the difference between ensuring the well-being of those sent into combat, or risking their loss because of the employment of procedures and tactics which do not optimize the coordinated capabilities of all the Services."[10] Let's now turn to a discussion on the significance of Service doctrine.

The Significance of Service Doctrine

The purpose of Service doctrine, more specifically Air Force doctrine, generally mirrors that of joint doctrine. According to AFDD 1, Air Force Basic Doctrine, Air Force doctrine:

> ...establishes general doctrinal guidance for the application of air and space forces in operations across the full range of military operations from global nuclear or conventional warfare to military operations other than war (MOOTW). It...should form the basis from which air commanders plan and execute their assigned air and space missions and act as a component of a joint or multinational force.[11]

As we saw above, the same two themes prevail when discussing the significance of Air Force doctrine. Like joint doctrine, Air Force doctrine embodies lessons learned from past training, exercises, and operations, and these lessons form the foundation for thinking about, planning, and executing future operations. Concerning lessons learned, AFDD 1 states:

> Air and space doctrine is a statement of officially sanctioned beliefs and warfighting principles that describe and guide the proper use of air and space forces in military operations. It is what we have come to understand, based on our experience to date...Doctrine consists of fundamental principles by which military forces guide their actions in support of national objectives. It is the linchpin of successful military operations, and Air Force doctrine is meant to codify accumulated wisdom...Air and space doctrine is an accumulation of knowledge gained primarily from the study and analysis of experience, which may include actual combat or contingency operations as well as equipment tests or exercises. As such, doctrine reflects what has usually worked best. In those less frequent instances in which experience is lacking or difficult to acquire (e.g., theater nuclear operations), doctrine may be developed through analysis of theory and postulated actions.[12]

Air Force Doctrine Document 1 goes on to explain that these beliefs, principles, accumulated wisdom, and gained knowledge provide:

> ...a common frame of reference on the best way to prepare and employ air and space forces. Accordingly, air and space doctrine shapes the manner in which the Air Force organizes, trains, equips, and sustains its forces. Doctrine prepares us for future uncertainties and, combined with our basic shared core values, provides a common set of understandings on which airmen base their decisions...[It is meant to provide] a framework for the way we prepare for, plan, and conduct air and space operations.[13]

To summarize, Air Force doctrine incorporates lessons learned from tests, training, exercises, and actual combat or contingency operations, and these lessons form the foundation for preparing, planning, and conducting air and space operations. We've seen that both Air Force doctrine and joint doctrine provide guidance for employing forces in ongoing or future operations. Since both Air Force and joint doctrine encapsulate these same general themes, we now ask ourselves; what's the relationship between Air Force doctrine and joint doctrine?

The Relationship between Air Force and Joint Doctrine

Although the US military has a successful history of fighting as a joint team, focus on joint doctrine development is relatively new. As JP 1-01.1 notes:

> Prior to 1986, no single individual or agency had overall responsibility for joint doctrine. As a result, there was no established process for the identification of critical joint doctrine voids and there were no procedures for participation by the combatant commands in the development of joint doctrine. There was also no single agency responsible for ensuring consistency between existing joint doctrine, Service doctrine, multi-Service doctrine, and combined doctrine.[14]

The Goldwater-Nichols Department of Defense Reorganization Act of 1986 changed all that. The Goldwater Nichols Act made the Chairman of the Joint Chiefs of Staff responsible for joint doctrine development.[15] This law spurned the development of several directives which further clarified the Chairman's new responsibilities. One of these directives, JCS Pub 2, established the relationship between Service and joint doctrine. It states, "Each Service will ensure that its doctrine and procedures are Consistent [sic] with joint doctrine established by the Chairman of the Joint Chiefs of Staff."[16] To further amplify the importance of this relationship, the policy documents JP 1, JP 1-01, and JP 1-01.1 all mention that Service doctrine must be consistent with joint doctrine.[17]

So far, we've looked at the significance of joint and Service doctrine and established what the relationship is between the two. Let's briefly look now at the development and relationship between AFDD 2-5 and JP 3-13.

AFDD 2-5 and JP 3-13

As stated in the introduction, AFDD 2-5 and JP 3-13 were developed concurrently between 1995 and 1998. Several studies have traced the evolutionary path of these two documents, so we won't repeat it here.[18] What is significant for this study is that AFDD 2-5 was finalized and

published on 5 August 1998, while JP 3-13 was finalized and published over 2 months later on 9 October 1998. As we've already seen, each Service is responsible for ensuring that its doctrine is consistent with joint doctrine. The mere fact that AFDD 2-5 came out earlier than JP 3-13 raises a fundamental question as to whether the Air Force pursued the appropriate actions to ensure consistency. If AFDD 2-5 is found to be inconsistent with JP 3-13, we'll explore whether there has been any negative impact to military operations at the strategic, operational, and/or tactical levels due to the inconsistency.

Notes

[1] Joint Pub (JP) 1-01, *Joint Doctrine Development System*, 5 July 2000, I-1.
[2] JP 1, *Joint Warfare of the Armed Forces of the United States*, 10 January 1995, I-3.
[3] JP 1-01, I-1.
[4] JP 1, I-3.
[5] Ibid., I-3 and I-4.
[6] JP 1-01, I-1.
[7] Ibid., I-1.
[8] JP 1-01.1, *Compendium of Joint Publications*, 23 April 1999, A-4.
[9] Ibid., A-3 and A-4.
[10] Ibid., A-5.
[11] Air Force Doctrine Document (AFDD) 1, *Air Force basic Doctrine*, September 1997, v.
[12] Ibid., 1 and 2.
[13] Ibid., 1.
[14] JP 1-01.1, A-2.
[15] Goldwater-Nichols Department of Defense Reorganization Act of 1986, 1 October 1986, 10 USC 153 (a)(5)(n).
[16] Joint Chiefs of Staff Pub 2, December 1986.
[17] JP 1, I-4; JP 1-01, I-2; and JP 1-01.1, A-2.
[18] Three such studies are: (1) Davis, Lt Col Harry J. "Developing Air Force Information Warfare Operational Doctrine: The Crawl-Walk-Run Approach." Research Report. Maxwell AFB, Alabama: Air War College, 1 April 1996. (2) Henning, Maj Paul R. "Air Force Information Warfare Doctrine: Valuable or Valueless? Research Report no. 97-0604C. Maxwell AFB, Alabama: Air Command and Staff College, March 1997. (3) Hollman, Capt Ryan D. *A Descriptive Study of Information Operations and Information Warfare Awareness in the United States Air Force*. Masters diss., Air Force Institute of Technology, September 1998.

Chapter 3

Issue Analysis

Doctrine [is] every action that contributes to unity of purpose...it is what warriors believe in and act on.

—Captain Wayne P. Hughes, Jr., USN, Fleet Tactics

As stated in the introduction, this research paper will analyze the consistency between AFDD 2-5 and JP 3-13 in three principal areas: the components of IS and definitions of the key terms IS, IO, and IW; Air Force addition of the terms CI, OCI, and DCI; and the capabilities and related activities used to carry out offensive and defensive IO. To facilitate our analysis, Figure 1 depicts the joint IS construct, while Figure 2 contains the Air Force IS construct. If AFDD 2-5 is found to be inconsistent with JP 3-13, we'll explore whether there has been any negative impact to military operations at the strategic, operational, and/or tactical levels due to this inconsistency. We'll begin by looking at the components of IS and key definitions.

The Components of Information Superiority and Key Definitions

To begin our discussion, let's take a look at how the joint world conceptualizes IS. In July of 1996, the Chairman of the Joint Chiefs of Staff issued Joint Vision 2010 (JV 2010) which provides a conceptual framework for America's armed forces to think about the future.[1] A short time later, the Joint Warfighting Center published Concept for Future Joint Operations,

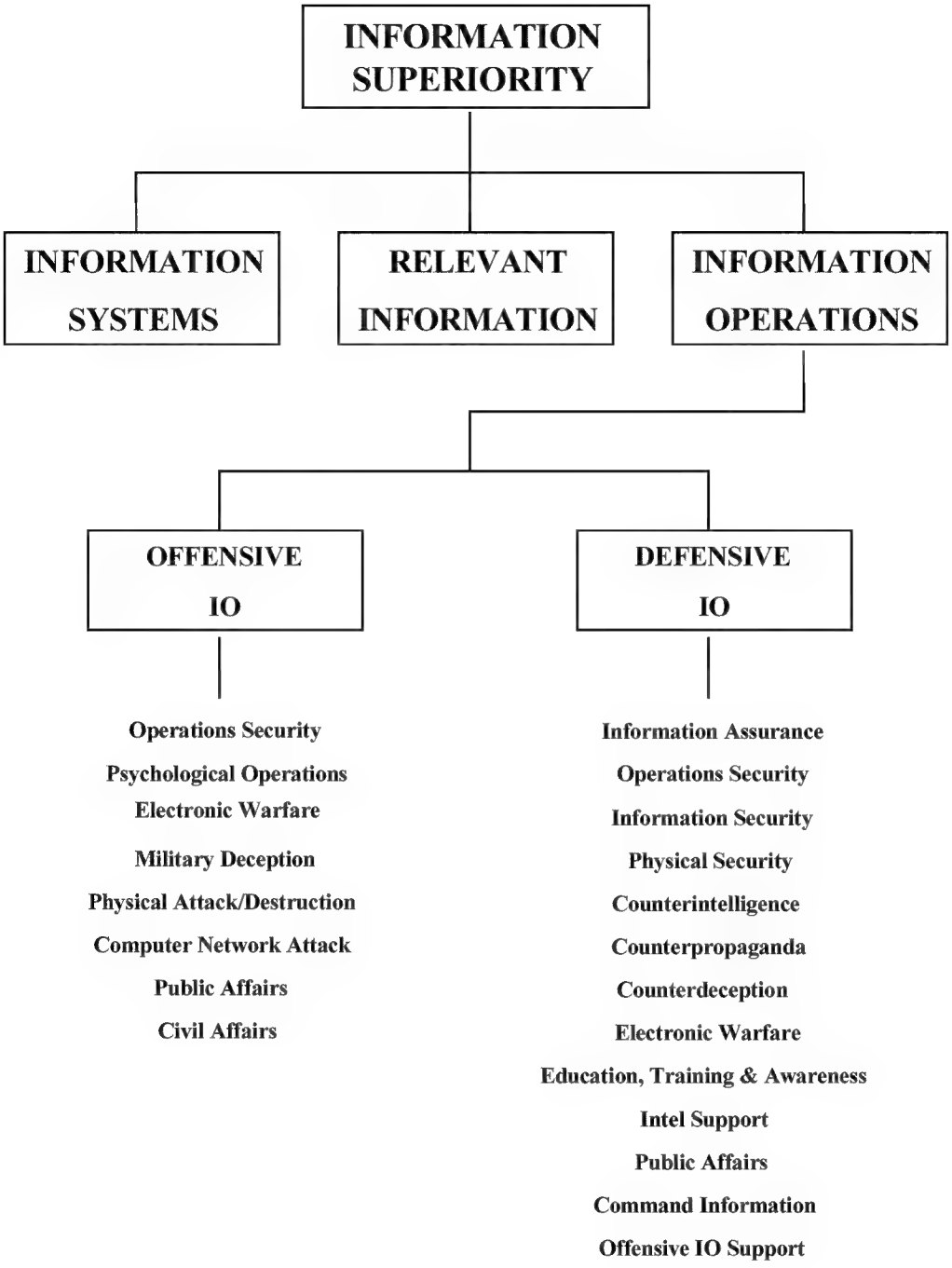

Figure 1. Joint Information Superiority Construct[2]

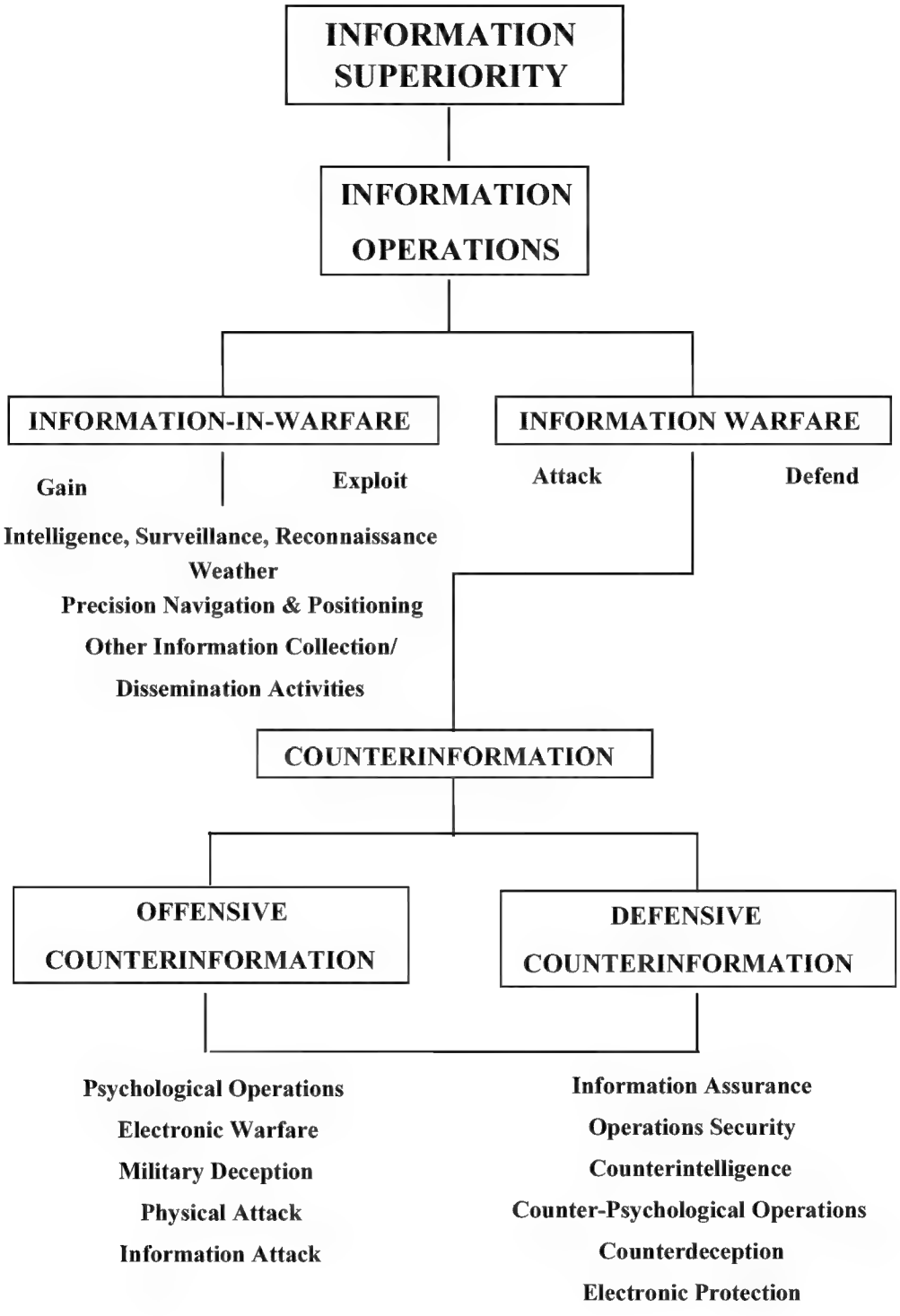

Figure 2. Air Force Information Superiority Construct[3]

Expanding Joint Vision 2010. This document explains that "JV 2010 is built on the premise that modern and emerging technologies--particularly information-specific advances--should make possible a new level of joint operations capability. Underlying a variety of technological innovations is information superiority."[4] Information superiority is defined as:

> ...the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.[5]

To expound on this concept, the document goes on to state that the three components of IS are information systems, relevant information, and IO.[6] Although the relationship between these components is depicted as three overlapping circles in the Concept document, we've depicted them in Figure 1 as a block diagram for simplicity's sake.

Joint Pub 3-13 acknowledges the term IS and its three components as follows:

> To achieve and sustain information superiority, Joint Force Commanders should integrate the following:
>
> - Activities that leverage friendly information systems, to include the friendly decision making process [i.e. Information Systems].
>
> - Intelligence and other information-related activities that provide them with timely, accurate, and relevant information on friendly forces, adversaries or potential adversaries, and the battlespace required to achieve their objectives [i.e. Relevant Information].
>
> - Offensive and defensive IO [i.e. Information Operations].[7]

Since we're interested in IO, we'll focus our attention there. According to JP 3-13, IO is defined as:

> ...actions taken to affect adversary information and information systems, while defending our own information and information systems...There are two major subdivisions within IO: offensive IO and defensive IO.[8]

Not depicted in the joint IS construct is the term "information warfare." The definition will clarify the reason why. Joint Pub 3-13 defines IW as:

> Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.[9]

As we can see, JP 3-13 makes a distinction between IO and IW based on a temporal relationship. Both concepts are identical, but the delineating factor is whether we are in a time of peace, crisis, or conflict. As we'll see next, the Air Force IS construct is quite different.

Just like the joint world, the Air Force recognizes that IS is the capstone term; however, the Air Force defines it differently. According to AFDD 2-5:

> The Air Force prefers to cast 'superiority' as a state of relative advantage, not a capability, and views information superiority as: 'That degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.'[10]

Air Force Doctrine Document 2-5 further states that "While information superiority is not solely the Air Force's domain, the strategic perspective and global experience gained from operating in the aerospace continuum make airmen uniquely prepared to gain and use information superiority through robust IO and execute its two major aspects: information-in-warfare (IIW) and information warfare (IW)."[11] The Air Force defines IO, IIW, and IW as follows:

> IO: The Air Force believes that in practice a more useful working definition is: 'Those actions taken to gain, exploit, defend or attack information and information systems and include both information-in-warfare and information warfare.'[12]
>
> IIW: Involves the Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on integrated intelligence, surveillance, and reconnaissance (ISR) assets; its information collection/dissemination activities; and its global navigation and positioning, weather, and communications capabilities.[13]
>
> IW: The Air Force believes that, because the defensive component of IW is always engaged, a better definition is: 'Information operations conducted to defend one's own information and information systems, or to attack and affect an adversary's information and information systems.'[14]

As we can see from Figures 1 and 2, and the definitions provided above, the joint IS construct and the Air Force IS construct are decidedly different. Let's look at these differences in greater detail.

When focusing on the components of IS and key definitions, there are essentially four areas of divergence. Starting at the top of Figures 1 and 2 and working our way down, we note the following differences:

1. The definitions for IS are different.
2. The components which make up IS are different.
3. The definitions and major subdivisions of IO are different.
4. The definitions for IW are different.

Table 1 below provides a side-by-side summary of definitions which should help us trace the arguments in the following analysis. First, we'll look at the definitions for IS.

A cursory look at the two definitions of IS reveals some similarities. Both definitions include the words "collect" and "exploit" when referring to friendly information capabilities, in addition to mentioning "defending" or "denying" an adversary's ability to affect our information. The major difference is that the joint world defines IS as absolute perfection; an "uninterrupted flow of information" on the friendly side, while denying an uninterrupted flow on the adversary side. The Air Force, on the other hand, recognizes that operations in the information realm won't be perfect, and prefers to look at IS as a state of "relative advantage." In other words, adversaries will attempt to disrupt IO, however, Air Force IS will ensure these attempts are ineffective. It's beyond the scope of this study to determine which of these definitions is correct. We can safely say, however, that the Air Force definition of IS is inconsistent with the joint definition.

The second area of divergence is the components that make up IS. As we can see in Figure 1, the joint IS components are information systems, relevant information, and IO. However, in Figure 2, the Air Force has only one IS component; IO. Suffice it to say that the

Table 1. Key Definitions

	Joint	Air Force
Information Superiority	The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.	That degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.
Information Operations	Actions taken to affect adversary information and information systems, while defending our own information and information systems...There are two major subdivisions within IO: offensive IO and defensive IO.	Those actions taken to gain, exploit, defend or attack information and information systems and include both information-in-warfare and information warfare.
Information Warfare	Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.	Information operations conducted to defend one's own information and information systems, or to attack and affect an adversary's information and information systems.

Sources: Joint Warfighting Center. *Concept for Future Joint Operations: Expanding Joint Vision 2010*, May 1997, i; JP 3-13, *Joint Doctrine for Information Operations*, 9 October 1998, I-9 and GL-7; and AFDD 2-5, *Information Operations*, 5 August 1998, 41 and 42.

difference between the joint world and Air Force in this respect is obvious. When we delve into the definitions of IO, the reasons for this inconsistency will become apparent.

The third area of divergence concerns the definitions and major subdivisions of IO. Referring to the definitions of IO in Table 1, we see that both definitions define IO as actions that affect or attack adversary information and information systems, while defending our own information and information systems. The difference lies in the Air Force addition of the terms "gain" and "exploit." In essence, the inclusion of these terms makes up for the absence of "information systems" and "relevant information" as components of IS. Put another way, the Air Force has combined the three joint IS components into one component, IO, which encompasses the gain, exploit, attack and defend activities. We should note, however, that the Air Force hasn't

completely eliminated the concepts behind "information systems" and "relevant information" from their construct. They've simply combined the terms, changed the name to IIW, and placed it under IO. The "attack" and "defend" pieces are now part of "information warfare" which is the other major subdivision under IO. This highlights another difference in the IO definitions.

Since the joint world included the "gain" and "exploit" pieces under IS, they made the two major subdivisions under joint IO offensive and defensive IO. These two subdivisions encompass the "attack" and "defend" pieces. On the other hand, the two major subdivisions under Air Force IO are information-in-warfare and information warfare. Let's turn now to the fourth and final area of divergence.

The first thing to note when comparing the definitions of joint and Air Force IW is that both start off by stating that IW is IO, however, the similarities end there. As noted earlier, JP 3-13 makes a distinction between IO and IW based on a temporal relationship. Both concepts are identical, but the delineating factor is whether we are in a time of peace, crisis, or conflict. Since the Air Force believes we're always in a state of IW because the defensive side is always engaged, they define IW as IO conducted to defend friendly information and information systems, or to attack and affect an adversary's information and information systems. For all intents and purposes, this definition is exactly the same as the joint IO definition. Again, it's not the purpose of this study to provide value judgements on which definition is right or wrong. We only note the inconsistency between the definitions. Let's continue our analysis by delving further down the joint and Air Force IS constructs represented in Figures 1 and 2. Our focus now turns to the Air Force addition of the terms CI, OCI, and DCI.

Air Force Addition of the Terms Counterinformation, Offensive Counterinformation, and Defensive Counterinformation

Referring to Figure 2, we can see under IW that the Air Force has decided to follow a common thematic template laid down in earlier Air Force doctrine for air and space operations. To be more specific, the Air Force chose to have IO functions follow the counterair/counterspace theme. Like counterair and counterspace, IW consists of the function CI and its two subsets, OCI and DCI. Air Force Doctrine Document 2-5 defines CI, OCI, and DCI as follows:

> CI: Counterinformation seeks to establish a desired degree of control in information functions that permits friendly forces to operate at a given time or place without prohibitive interference by the opposing force.[15]
>
> OCI: Offensive IW activities which are conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems.[16]
>
> DCI: Activities which are conducted to protect and defend friendly information and information systems.[17]

While the term CI is consistent with other Air Force doctrine concepts, it is inconsistent with the joint construct. Basically, we see that the Air Force has returned to a theme previously described in the definition of IS; that of relative advantage. It's this very concept that sets the Air Force apart from the joint world. Having noted this difference, let's compare the definitions of the joint terms offensive IO and defensive IO with OCI and DCI. Just as we did in the previous section, Table 2 below provides a side-by-side summary of definitions which should help us trace the arguments in the following analysis. When comparing the definitions of joint offensive IO to Air Force OCI, there are two major differences. The most notable difference is the objective that these activities hope to achieve. In the case of offensive IO, assigned and supporting capabilities and activities attempt to "affect adversary decisionmakers to achieve or promote specific objectives," while in the case of OCI, offensive IW activities are conducted to

Table 2. Offensive IO, Defensive IO, OCI and DCI Definitions

	Joint		Air Force
Offensive IO	The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decisionmakers to achieve or promote specific objectives. These capabilities and activities include, but are not limited to operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could include computer network attack...Other activities that may contribute to offensive IO include, but are not limited to, public affairs and civil affairs.	**OCI**	Offensive IW activities which are conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems.
Defensive IO	Defensive IO integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive IO are conducted through information assurance, information security, physical security, operations security, counterdeception, counterpropaganda, counterintelligence, electronic warfare and special information operations...Other activities that contribute to defensive IO include education, training, and awareness; intelligence support; public affairs, command information and offensive IO support.	**DCI**	Activities which are conducted to protect and defend friendly information and information systems.

Sources: JP 3-13, *Joint Doctrine for Information Operations*, 9 October 1998, GL-7 and II-6 and AFDD 2-5, *Information Operations*, 5 August 1998, 16 and 17.

"control the information environment." The other difference is that joint offensive IO lists the more prominent capabilities and activities that will be used to achieve specific objectives. Air Force OCI, on the other hand, describes the effects that offensive activities will have on adversary information and information systems in order to control the information environment.

Referring to the defensive definitions, joint defensive IO and Air Force DCI are essentially the same. Both definitions state that defensive activities "protect and defend information and information systems." The only difference is that the joint definition goes into detail as to the activities used to carry out defensive IO.

As mentioned in the previous section, it's not the purpose of this study to make value judgements on which definitions are right or wrong. Other than the similarity between the definitions for defensive IO and DCI, this section also shows inconsistencies between the Air Force and joint constructs. Let's now turn to the bottom of Figures 1 and 2 and compare capabilities and related activities.

Capabilities and Related Activities

In this section, we'll compare the capabilities and related activities used by the joint world and Air Force to conduct IO. Referring to Figures 1 and 2, we'll begin by comparing the activities on the offensive side. The first thing we'll note is the similarities. As you can see, both the joint world and Air Force use psychological operations (PSYOP), electronic warfare (EW), military deception, and physical attack to conduct offensive IO. In the case of PSYOP, EW, and military deception, the Air Force has adopted the joint definitions. For physical attack/destruction, the definitions are essentially the same. The joint world defines physical attack/destruction as "the use of 'hard kill' weapons against designated targets as an element of an integrated IO effort."[18] The Air Force defines physical attack as "The means to disrupt, damage,

or destroy information systems through the conversion of stored energy into destructive power."[19] Let's take a look now at the differences.

As far as differences go, we can see that under OCI, the Air Force doesn't consider operations security (OPSEC) an offensive IO capability. Traditionally, OPSEC has been thought of as a defensive capability, and both Air Force and joint IO doctrine acknowledge this fact by including OPSEC on the defensive side. Joint Pub 3-13 offers an explanation why OPSEC is included under offensive IO: "Some [offensive and defensive] capabilities or activities appear more offensive or defensive in nature, but it is their integration and potential synergy that ensures successful offensive and defensive IO."[20] Concerning OPSEC, JP 3-13 states that:

> OPSEC contributes to offensive IO by slowing the adversary's decision cycle and providing opportunity for easier and quicker attainment of friendly objectives...OPSEC denies the adversary critical information about friendly capabilities and intentions needed for effective and timely decision making, leaving the adversary vulnerable to other offensive capabilities "[21]

Whether OPSEC belongs under offensive IO or not is irrelevant to our discussion. We again simply note that Air Force IO doctrine is different than joint doctrine in this respect.

The next discrepancy we see is that the Air Force has added a new term to the IO lexicon; information attack. Information attack is defined as, "An activity taken to manipulate or destroy an adversary's information systems without visibly changing the physical entity within which it resides."[22] On the joint side, however, the term "computer network attack" comes closest to information attack. Computer network attack (CNA) is defined as, "Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[23] The apparent difference between the two terms is that CNA takes into account physical destruction of computers and computer networks, whereas information attack stresses that the physical entity within which an information system resides remains unaffected.

Next, we note that public affairs (PA) and civil affairs (CA) are missing under OCI. The inclusion of PA as an IO capability has been, and continues to be, a very controversial subject. This controversy is best summed up by 2d Lt David Englin in his Harvard thesis, The Lightning Bolt and the Quill: Determining the Role of Air Force Public Affairs in Information Warfare.[24] After examining DOD Directive 5122.5, DOD Principles of Information, JP 3-53, Doctrine for Joint Psychological Operations, JP 3-58, Joint Doctrine for Military Deception, and JP 3-61, Doctrine for Public Affairs in Joint Operations, Englin found that they explicitly constrain the potential IO role of public affairs.[25] He summarizes these constraints as follows: quickly and completely release all information; never release any kind of misinformation; the only valid reasons for restricting or withholding information are national or operational security and the safety and privacy of personnel; and do not manipulate public opinion.[26] As Englin notes, the first three constraints are reasonable and important for protecting democratic accountability. Furthermore, he states that "the most important asset public affairs has is its credibility. If audiences fail to believe the information released by public affairs, then public affairs loses its value...The first three constraints are necessary to preserve that credibility."[27] The fourth constraint is where the crux of the controversy lies. A significant number of public affairs officers (PAOs) believe that terms like "influence" and "manipulate" undermine the credibility of public affairs, and hence they tend to be vocal advocates for avoiding any association with IO. Englin explains:

> Perhaps the difference between *influencing* and *manipulating* key audiences is more than semantic. The pejorative implications of the term *manipulating* may suggest an element of deceit. If attempting to *manipulate* an audience inherently requires some form of deceit, then it would violate the principles of openness and honesty which guide public affairs and protect its credibility. If, on the other hand, attempting to *influence* an audience means targeted communication of messages which are open, honest, and factual, then such activities would be well within the bounds of legal and moral constraints placed on public affairs.[28]

After much debate at both the Air Force and joint levels, the joint world included PA as an offensive IO "related activity," while the Air Force chose to avoid inclusion. We should note here that in the latest draft version of the updated AFDD 2-5 dated September 2000, PA operations are included under IIW, and the document readily acknowledges that "public affairs operations influence decision-making of foreign leaders by making international audiences aware of forces being positioned and US resolve to employ those assets."[29]

The exclusion of civil affairs from OCI is much less controversial. The Air Force simply doesn't possess any dedicated active duty civil affairs assets; however, there are 248 Air Force Reserve lawyers who exclusively support Army civil affairs missions.[30] The Air Force apparently felt this capability wasn't significant enough to warrant inclusion under OCI. We now turn to the defensive side.

On the defensive side, we can also see several similarities between Air Force and joint doctrine. Both the joint world and Air Force use information assurance (IA), OPSEC, counterintelligence (CI), and counterdeception to conduct defensive IO. The Air Force has adopted the joint definitions for IA, OPSEC, and counterdeception, while the definitions for CI are technically different, but basically the same. The joint world defines CI as "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."[31] The Air Force, on the other hand, states that CI "protects operations, information, systems, technology, facilities, personnel, and other resources from illegal clandestine acts by foreign intelligence services, terrorist groups, and other elements."[32] Let's now look at the differences.

Looking at the differences, we notice under DCI that information security (INFOSEC); physical security (PHYSEC); education, training and awareness; intel support; PA; command information; and offensive IO support are all missing. Although not specifically addressed under DCI, intel support, PA, and command information are mentioned elsewhere in AFDD 2-5 as supporting DCI.[33] We should also note that the Air Force includes one of three electronic warfare subdivisions, "electronic protection," rather than the all inclusive term "electronic warfare." After exhaustive research, the author was unable to find any specific reason for the total omission of INFOSEC; PHYSEC; education, training and awareness; and offensive IO support; and use of the term electronic protection versus electronic warfare.

Another difference noted is that the Air Force uses the term counterPSYOP instead of the joint term counterpropaganda. Although counterPSYOP is not specifically defined in AFDD 2-5, the document states that "Numerous organizations and activities (for example, intelligence, surveillance, and reconnaissance (ISR), military units, and commanders) can identify adversary psychological warfare operations attempting to influence friendly populations and military forces. Countering such messages is vital to successful operations."[34] Like AFDD 2-5, JP 3-13 doesn't specifically define counterpropaganda, but states that "Activities identifying adversary propaganda contribute to situational awareness and serve to expose adversary attempts to influence friendly populations and military forces."[35] To further analyze this disparity, let's take a look at the definitions of psychological operations and propaganda.

Joint Pub 1-02 defines psychological operations as: "Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes

and behavior favorable to the originator's objectives."[36] Both JP 3-13 and AFDD 2-5 have adopted this definition. As far as propaganda is concerned, neither JP-3-13 nor AFDD 2-5 includes a definition of the term. Joint Pub 1-02, however, defines it as "Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly."[37] On the surface, both definitions appear to be identical, however, if we look at JP 3-53, Doctrine for Joint Psychological Operations, it states that, "PSYOP techniques are used to plan and execute truth projection activities intended to inform foreign groups and populations persuasively."[38] Since PSYOP executes truth projection, and propaganda can be "any form of communication" (including falsehoods), it would appear the Air Force is saying that they will counter adversary truths designed to influence our emotions, motives, objective reasoning, and ultimately our behavior rather than adversary propaganda, which would include both truths and falsehoods. Whether this was the intention of the Air Force is not known.

To summarize, both similarities and differences exist between the capabilities and related activities used by the Air Force and joint world to conduct IO. As far as similarities are concerned, we saw that both joint and Air Force IO doctrine include PSYOP, EW, military deception, and physical attack on the offensive side. On the defensive side, both doctrines include IA, OPSEC, CI, and counterdeception. As far as differences go, the Air Force chose to omit OPSEC, PA, and CA on the offensive side, while introducing the term information attack. Defensively, the Air Force specifically omits INFOSEC; PHYSEC; education, training and awareness; intel support; PA; command information; and offensive IO support, while including electronic protection and counterPSYOP. Despite the similarities noted in this section, the omission of some activities by the Air Force, along with the introduction of new terms,

contributes to the overall inconsistency between joint and Air Force doctrine. We now turn to an overall summary of our analysis.

Is AFDD 2-5 Consistent with JP 3-13?

Overall, Air Force IO doctrine is inconsistent with joint IO doctrine. In this chapter, we examined this inconsistency in three principal areas. In the first area which looked at the components of IS and key definitions, we noted four areas of divergence. In Figures 1 and 2 from the top down, we noted that:

1. The definitions for IS are different.
2. The components which make up IS are different.
3. The definitions and major subdivisions of IO are different.
4. The definitions for IW are different.

In the second area, we noted that the term CI is consistent with other Air Force doctrine concepts, however, it's inconsistent with joint doctrine. When comparing the definitions of the joint terms offensive IO and defensive IO with Air Force OCI and DCI, we found that the offensive definitions were inconsistent, however, the defensive definitions were virtually identical. Despite this similarity, this section also showed inconsistencies between Air Force and joint doctrine.

In the final area, we compared the capabilities and related activities the Air Force and joint world use to conduct IO. While similarities exist, the omission of some activities by the Air Force, along with the introduction of new terms, contributes to the overall inconsistency. Having shown that AFDD 2-5 is inconsistent with JP 3-13, we now explore whether there has been any negative impact to military operations at the strategic, operational, and/or tactical level due to the inconsistency.

Strategic, Operational, and/or Tactical Level Impact

To determine whether there has been a negative impact to military operations, we have a single significant event to analyze: Operation ALLIED FORCE. This was the first time a comprehensive IO campaign was incorporated into a major conflict.[39] Operation ALLIED FORCE was a success for NATO. However, one doctrinal disconnect appears to have caused significant problems, the absence of PA as an offensive or defensive activity in Air Force IO doctrine. Before we examine this subject, let's begin by looking at which IO organizations were involved in ALLIED FORCE.

In mid-1998, early indications of an impending catastrophe in the Balkans prompted Supreme Headquarters Allied Powers Europe to begin planning for military operations against Serbia.[40] Since NATO had neither IO doctrine nor an IO organization, IO planning was accomplished by the EUCOM IO Cell.[41] The USAFE IW Flight, which is part of this cell, contributed the Air Force portion of the plan[42]. Although details of the final plan are classified, we do know that EUCOM PA was integrated with IO in accordance with JP 3-13.[43] By the spring of 1999, evidence was mounting that Slobodan Milosevic was conducting a systematic campaign of forced relocations and ethnic cleansing in Kosovo. NATO decided to respond. According to a U.S. Air Force report:

> A number of ground options were considered, but none were taken past the level of contingency planning. The decision was ultimately reached to pursue NATO's objectives exclusively through an air campaign...This was to be the second major use of NATO air assets against Serb forces; the first was NATO's limited but successful operation over Bosnia in 1995 (Operation Deliberate Force). Alliance leaders were hoping for a similarly quick result this time: Serbia's capitulation after a modest set of air strikes to show NATO resolve.[44]

Since NATO believed the air campaign would be short, they decided to send the EUCOM IO Cell home.[45] However, the USAFE IW Flight remained in Italy to execute their portion of the

IO plan in support of the air campaign.[46] This plan was based on AFDD 2-5 and did not include PA integration with IO.[47] Why is this significant?

Public Affairs has played an increasingly important role in modern conflicts. One of the major lessons of the Vietnam War was the indelible impact the media had on public opinion and military operations. In his article entitled Tactical-Level Public Affairs and Information Operations, Army Major Mark R. Newell illustrates this point:

> ...near real-time media reporting and analysis of tactical and operational military actions can have expeditious effects at the strategic level. This impact, and consequent shifts in national and military strategies or policies, is known as the 'CNN effect.' TV viewers, including leaders, react emotionally and forcefully to images, and public pressure forces policy makers to respond quickly...Therefore, media coverage can be pivotal to the success of the operation and achieving national strategic goals.[48]

Knowing that U.S. and Western publics are sensitive to casualties (both military and civilian) and collateral damage, adversaries have facilitated media coverage of these indiscretions and blamed them on friendly military operations. Milosevic used this very template during Operation ALLIED FORCE. According to an Air University report:

> ...Milosevic took the offensive in the public affairs war by exploiting numerous propaganda opportunities, to which NATO had to react. After the initial attacks, it became apparent that Milosevic was attempting to divide the NATO alliance by waging a propaganda war. Milosevic took every opportunity to publicize each incident of civilian casualties caused (or supposedly caused) by NATO bombing. As a result of casualties and incidents of collateral damage early in the war, negative public reaction followed and targeting temporarily became even more restrictive.[49]

Admiral James Ellis, Commander of Joint Task Force Noble Anvil during Operation ALLIED FORCE, concludes that "the enemy was much better at this [public information and public affairs] than we were...and far more nimble. The enemy deliberately and criminally killed innocents by the thousands, but no one saw it...We accidentally killed innocents, sometimes by the dozens, and the world watched on the evening news. We were continuously reacting,

investigating, and trying to answer 'how could this happen?'"[50] To avoid this pitfall in future conflicts, PA must be integrated with IO.

The integration of PA into an IO campaign can successfully counter media-savvy adversaries. As Air Force Major Gary Pounder states in his article "Opportunity Lost: Public Affairs, Information Operations, and the Air War Against Serbia:"

> Public Affairs--through its public information mission--can clearly supply some of the capital required for winning the media war (as part of the IO campaign) and can bolster public support for the overall military effort. However, successful integration of public information into IO remains problematic; although IO planners and Public Affairs Officers clearly had designs for what they hoped to accomplish during Allied Force, the doctrinal foundation for incorporating public information into IO remained unprepared for the challenges at hand.[51]

Despite the lack of definitive doctrinal guidance, IO planners and PA officers (PAOs) still attempted to integrate PA into the ALLIED FORCE IO campaign.[52] According to Pounder, "When USAFE's IO cell began active planning for the air campaign in December 1998, the command's PA staff was invited to participate; senior PAOs attended several IO planning meetings, but these sessions produced little in the way of specific public-information objectives for the planned IO campaign."[53] Attempts didn't stop there. Pounder elaborates: "Another IO planner claims that the IO staff approached PA about the possibility of public information as a 'deterrent factor' in January 1999--almost two months before the operation began. According to the IO specialist, PA appeared 'uninterested in the idea,' and the proposal quickly died."[54] Divorced from the IO effort, the Alliance's public-information strategy lacked the synergy that would have resulted through coordination with other IO initiatives.[55]

To summarize, the absence of PA as an offensive or defensive activity in Air Force IO doctrine had negative impact at the strategic, operational, and tactical levels. At the strategic level, an opportunity was lost to deter Milosevic before ALLIED FORCE ever began. As we saw, the USAFE IW Flight attempted to engage PA in such activities but they refused to get

involved. Another impact at the strategic level was the negative public reaction to casualties and collateral damage. By allowing Milosevic to exploit these opportunities unopposed, NATO lost its credibility. As part of an integrated IO campaign, PA must have a preemptive and reactive plan ready to go in anticipation of casualties and collateral damage. In addition, PA could've bolstered public support for the operation with open, honest and factual messages. At the operational level, Admiral Ellis noted that NATO was continuously reacting, investigating, and trying to answer questions of how casualties and collateral damage could happen. Scarce combat resources can certainly be better utilized fighting wars than investigating adversary propaganda charges. Again, an integrated IO campaign which includes a proactive PA plan could've thwarted Milosevic's efforts. Finally, at the tactical level, negative public reaction to casualties and collateral damage early in the war led to greater restrictions on targeting. The PA efforts cited above could've prevented this from happening. Research of unclassified sources only revealed the absence of PA as an offensive or defensive activity in Air Force IO doctrine as causing problems during ALLIED FORCE. As we saw earlier in this paper, there are other inconsistencies which have the potential to cause problems in future operations. These potential impacts are highlighted in Appendix A.

Notes

[1] Chairman of the Joint Chiefs of Staff. *Joint Vision 2010*, July 1996, 1.

[2] Joint Warfighting Center. *Concept for Future Joint Operations: Expanding Joint Vision 2010*, May 1997, 39 and Joint Pub 3-13, *Joint Doctrine for Information Operations*, 9 October 1998, II-1.

[3] Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, 5 August 1998, Figure 1.1, 3.

[4] Concept for Future Joint Operations: Expanding Joint Vision 2010, i.

[5] Ibid., i.

[6] Ibid., 39.

[7] Joint Pub (JP) 3-13, *Joint Doctrine for Information Operations*, 9 October 1998, I-2.

[8] Ibid., I-9.

[9] Ibid., GL-7.

Notes

[10] AFDD 2-5, 41
[11] Ibid., 2.
[12] Ibid., 41.
[13] Ibid., 41.
[14] Ibid., 42.
[15] Ibid., 40.
[16] Ibid., 42.
[17] Ibid., 40.
[18] JP 3-13, II-5.
[19] AFDD 2-5, 43.
[20] JP 3-13, II-3.
[21] Ibid., II-3.
[22] AFDD 2-5, 41.
[23] JP 3-13, GL-5.
[24] Englin, 2d Lt David L. *The Lightening Bolt and the Quill: Determining the Role of Air Force Public Affairs in Information Warfare*. Masters diss., Harvard University, 1998.
[25] Ibid., i.
[26] Ibid., 17.
[27] Ibid., 17.
[28] Ibid., 18.
[29] AFDD 2-5 (DRAFT), *Information Operations*, September 2000, 34.
[30] Conversation with USAF Major Fred Van Cleave, USAF representative on the joint doctrine working party for Joint Pub 3-57, *Doctrine for Joint Civil Affairs*. July 2000.
[31] JP 3-13, GL-5.
[32] AFDD 2-5, 18.
[33] Intelligence Support, AFDD 2-5, 21; Public Affairs, AFDD 2-5, 18; Command Information, AFDD 2-5, 18.
[34] AFDD 2-5, 18.
[35] JP 3-13, III-7.
[36] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 23 March 1994 as amended through 6 April 1999, 358.
[37] Ibid., 356.
[38] JP 3-53, *Doctrine for Joint Psychological Operations*, 10 July 1996, I-5.
[39] Pounder, Maj Gary. "Opportunity Lost: Public Affairs, Information Operations, and the Air War Against Serbia." *Airpower Journal*, Volume XIV, No. 2 (Summer 2000): 58.
[40] Department of the Air Force. *The Air War Over Serbia, Aeropace Power in Operation Allied Force*. Washington, D.C., April 2000, 5.
[41] Conversation with U.S. Air Force Lt Col Paul Bowman, EUCOM IO Cell Chief, March 2000.
[42] Pounder, 59.
[43] Conversation with U.S. Air Force Lt Col Paul Bowman, EUCOM IO Cell Chief, March 2000.
[44] The Air War Over Serbia, Aeropace Power in Operation Allied Force, 5.

Notes

[45] Conversation with U.S. Air Force Lt Col Paul Bowman, EUCOM IO Cell Chief, March 2000.

[46] Pounder, 59

[47] Ibid., 59.

[48] Newell, Maj Mark R. "Tactical-Level Public Affairs and Information Operations." *Military Review*, no. 6 (December 1998-February 1999): 22.

[49] Air University. *Response to "The Air War Over Serbia" Initial Report*. Maxwell AFB, Alabama, May 2000. In United States. Air Command and Staff College. *Joint Forces and Capabilities*. Maxwell AFB, Alabama, January 2001, 243.

[50] Pounder, 58.

[51] Ibid., 58.

[52] Ibid., 64.

[53] Ibid., 64.

[54] Ibid., 64.

[55] Ibid., 61 & 72.

Chapter 4

Summary/Conclusions/Recommendations

> *Doctrine establishes a particular way of thinking about war and a way of fighting...doctrine provides the basis for harmonious actions and mutual understanding.*
>
> —Fleet Marine Force Manual 1, Warfighting

In this research paper, we examined whether AFDD 2-5, Information Operations, is consistent with JP 3-13, Joint Doctrine for Information Operations, as required by policy directives.[1] Our analysis focused on consistency in three principal areas: the components of IS and definitions for the key terms IS, IO, and IW; Air Force addition of the terms CI, OCI, and DCI; and the capabilities and related activities used to carry out offensive and defensive IO. In the first area which looked at the components of IS and key definitions, we noted four inconsistencies. Starting at the top of Figures 1 and 2 and working down, we noted that the definitions for joint and Air Force IS are different; the components which make up IS are different; the definitions and major subdivisions of IO are different; and finally, the definitions for IW are different.

In the second principal area concerning Air Force addition of the terms CI, OCI, and DCI, we noted that CI is consistent with other Air Force doctrine concepts, however, it's inconsistent with joint doctrine. Referring to Table 2, we then compared the definitions of the joint terms offensive IO and defensive IO with Air Force OCI and DCI. Our analysis concluded that the

offensive definitions were inconsistent, however, the defensive definitions were virtually identical. Despite this similarity, this section also showed inconsistencies between Air Force and joint doctrine.

In the final principal area, we compared the capabilities and related activities the Air Force and joint world use to conduct IO. While similarities do in fact exist, the omission of some activities by the Air Force, along with the introduction of new terms, contributes to the overall inconsistency between joint and Air Force IO doctrine. Overall, we came to the conclusion that AFDD 2-5 is inconsistent with JP 3-13.

Having shown that Air Force and joint IO doctrine are inconsistent, we then asked whether there has been any negative impact to military operations at the strategic, operational, and/or tactical levels due to the inconsistency. To answer this question, we looked at Operation ALLIED FORCE. Research of unclassified sources only revealed the absence of public affairs (PA) as an offensive or defensive activity in Air Force IO doctrine as causing significant problems. The potential impact of other doctrinal inconsistencies on future operations is highlighted in Appendix A.

As previously mentioned, the Air Force has updated AFDD 2-5 and is presently soliciting comments on its web site before going final.[2] The Air Force IS construct found in this draft version has changed in only one respect; PA was added under IIW. If this draft version is adopted, it too will be inconsistent with joint IO doctrine. To reconcile the inconsistencies between Air Force IO doctrine and joint doctrine, two alternative Air Force IS constructs are offered. In the first alternative, depicted in Figure 3, the Air Force could simply adopt the joint IS construct including definitions. Looking at the components of IS, we see that the capabilities previously found under IIW would now come under relevant information. Moving to the bottom

of Figure 3, we note that compensation would be made for the lack of a significant Air Force CA capability by omitting it from the construct. I recommend the Air Force Doctrine Center adopt this construct since consistency questions would be virtually eliminated.

In the second alternative construct, depicted in Figure 4, the Air Force could retain some of its unique IO identity. To ensure consistency with joint IO doctrine, however, the Air Force would adopt the joint definitions for IS, information systems, IO, IW, offensive IO, and defensive IO. Referring to the components of IS, we see that "information support" has replaced "relevant information." The definition for information support would be the same as that for IIW. The reason we don't use the term IIW is because the joint world, unlike the Air Force, doesn't believe we're always in a state of information warfare. As a result, the word "warfare" would be inappropriate to connote peacetime IO. The next area of change is under offensive IO. As we can see, OPSEC and CA have been omitted. On the defensive side, we note that INFOSEC and PHYSEC have been omitted, while the term counterpropaganda replaces counterPSYOP, and electronic protection replaces electronic warfare. Since current Air Force IO doctrine mentions that intel support, public affairs, and command information support DCI, we've retained them in this construct. On both the offensive and defensive sides, the joint definitions would be adopted to bolster the argument of consistency.

By adopting one of these alternative IS constructs, the Air Force would ensure the consistency requirement of JCS Pub 2, JP 1, JP 1-01, and JP 1-01.1 is satisfied. More importantly, any negative strategic, operational, and/or tactical level impact, like those illustrated during Operation ALLIED FORCE, would be less likely to occur.

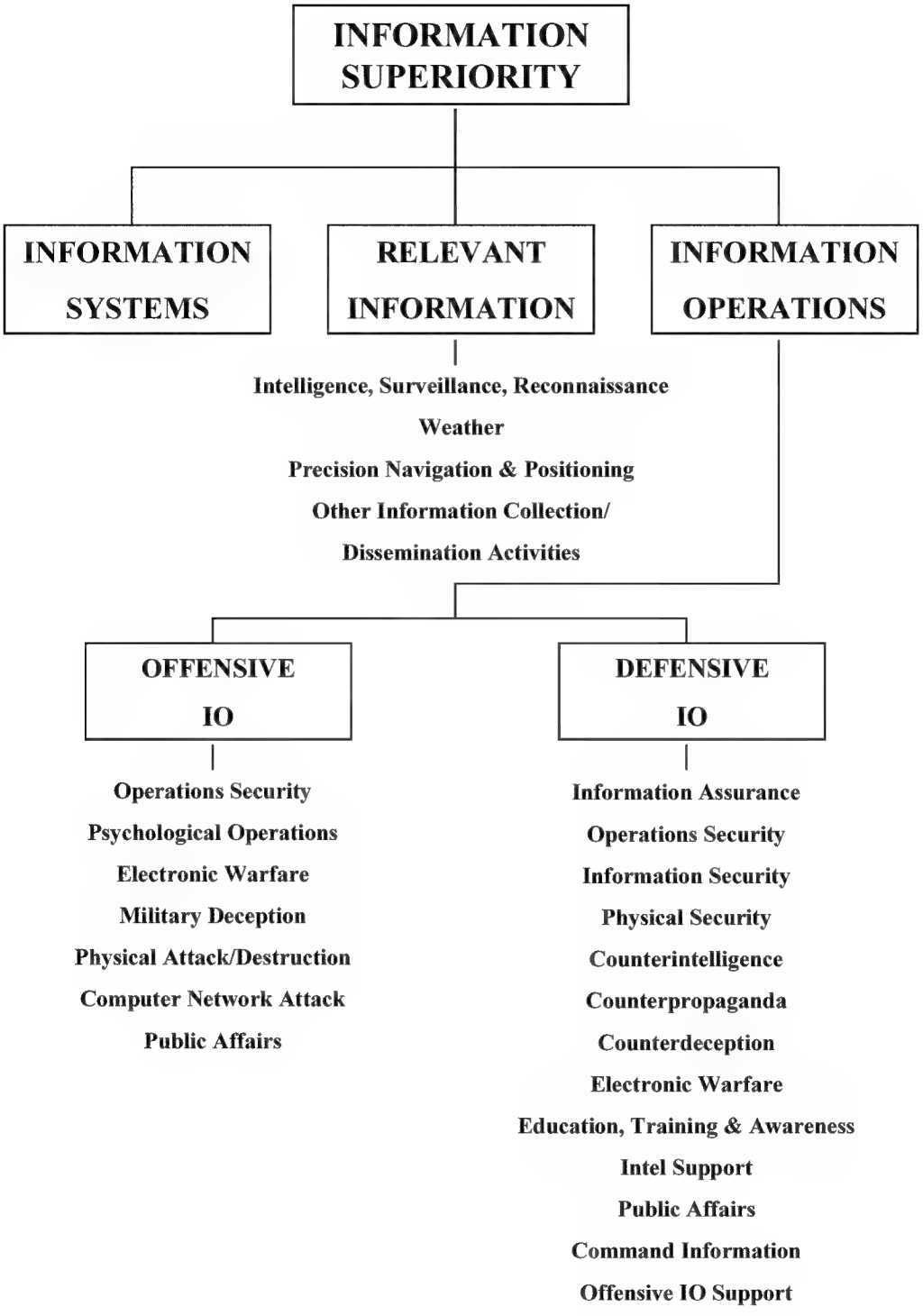

Figure 3. Air Force Information Superiority Construct--Alternative #1

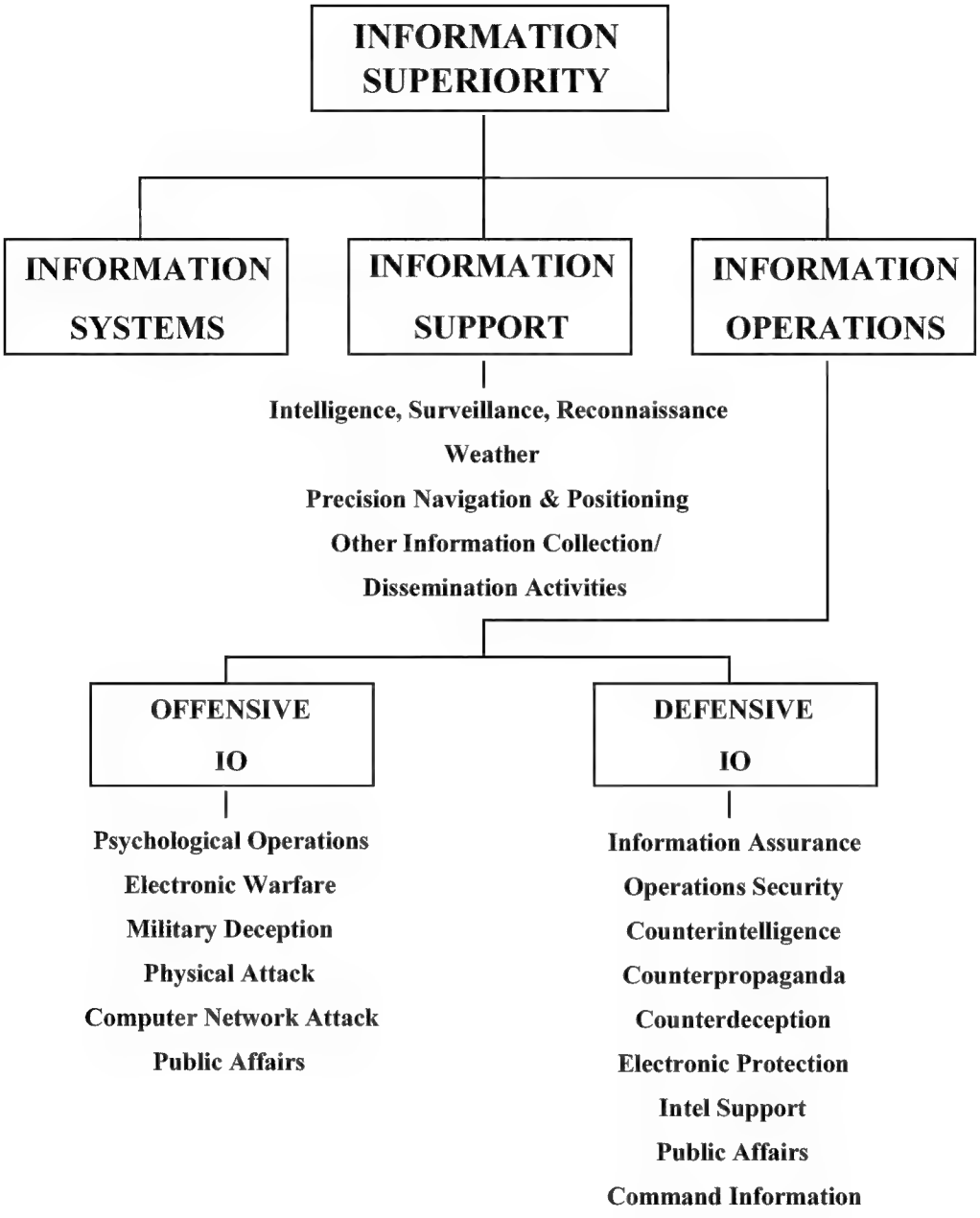

Figure 4. Air Force Information Superiority Construct--Alternative #2

Notes

[1] These policy directives are: Joint Chiefs of Staff Pub 2; Joint Pub (JP) 1, *Joint Warfare of the Armed Forces of the United States*, 10 January 1995; JP 1-01, *Joint Doctrine Development System*, 5 July 2000; and JP 1-01.1, *Compendium of Joint Publications*, 23 April 1999.

[2] The draft version of the updated AFDD 2-5 can be found at www.afdc.af.mil.

Appendix A

Potential Impact from Doctrinal Differences

The following table outlines the potential impact from doctrinal differences between Air Force Doctrine Document 2-5, Information Operations, and Joint Pub 3-13, Joint Doctrine for Information Operations.

Table 3 Potential Impact from Doctrinal Differences

Difference	Joint	Air Force	Potential Impact
Definitions for IS are Different	The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.[1]	That degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.[2]	1. Confusion in the joint IO Cell as joint planners continue toward goal of uninterrupted flow and denying it to adversaries while Air Force planners reallocate assets because relative advantage is achieved.
Components which Make Up IS are Different	Information Systems, Relevant Information, and Information Operations[3]	Information Operations[4]	1. Confusion in the joint IO Cell as Air Force planners attempt to integrate global awareness (IIW) capabilities into the joint IO plan.
Definitions and Major Subdivisions of IO are Different	Actions taken to affect adversary information and information systems, while defending our own information and information systems... There are two major subdivisions within IO: offensive IO and defensive IO.[5]	Those actions taken to gain, exploit, defend or attack information and information systems and include both information-in-warfare and information warfare.[6]	1. Confusion in the joint IO Cell as Air Force planners attempt to integrate gain and exploit (IIW) activities into the joint IO plan. 2. Confusion in the peacetime joint IO Cell as Air Force planners attempt to integrate "wartime" (IW and IIW) actions into the joint IO plan.

Difference	Joint	Air Force	Potential Impact
Definitions for IW are Different	Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.[7]	Information operations conducted to defend one's own information and information systems, or to attack and affect an adversary's information and information systems.[8]	1. Confusion in the joint IO Cell as the definitions for joint IO and Air Force IW are nearly identical.
Air Force addition of the term CI	No comparable term	Counterinformation seeks to establish a desired degree of control in information functions that permits friendly forces to operate at a given time or place without prohibitive interference by the opposing force.[9]	1. Confusion in the joint IO Cell as Air Force planners introduce a term unique to the Air Force.
Definition for joint offensive IO is different from definition for Air Force offensive counterinformation	The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decisionmakers to achieve or promote specific objectives.[10]	Offensive IW activities which are conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems.[11]	1. Confusion in the joint IO Cell as joint planners focus effects-based targeting on adversary decisionmakers while Air Force planners focus on information and information systems.

Difference	Joint	Air Force	Potential Impact
Air Force omission of OPSEC from the offensive side	OPSEC contributes to offensive IO by slowing the adversary's decision cycle and providing opportunity for easier and quicker attainment of friendly objectives...OPSEC denies the adversary critical information about friendly capabilities and intentions needed for effective and timely decision making, leaving the adversary vulnerable to other offensive capabilities.[12]	No doctrinal explanation.	1. Negligible impact since the joint world and Air Force include OPSEC on the defensive side.
Air Force addition of Information Attack on the offensive side	Computer Network Attack: Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.[13]	An activity taken to manipulate or destroy an adversary's information systems without visibly changing the physical entity within which it resides.[14]	1. Confusion in the joint IO Cell as joint planners assume Information Attack includes physical destruction of adversary information systems.

Difference	Joint	Air Force	Potential Impact
Air Force omission of Public Affairs from the offensive side	PA activities: (1) Expedite the flow of accurate and timely information to internal (own organization) and external (the public) audiences. (2) Create an awareness of the military goals during a campaign or operation. (3) Satisfy the desires of the internal and external audiences to be kept informed about the campaign or operation. (4) Inform internal and external audiences of significant developments affecting them. (5) Through the public media, allow a JFC to inform an adversary or a potential adversary about the friendly force's intent and capability. PA activities will not be used as a military deception capability or to provide disinformation to either internal or external audiences.[15]	No doctrinal explanation for omission.	1. Lack of synergy that would result from not coordinating and deconflicting Air Force PA with other IO initiatives.

Difference	Joint	Air Force	Potential Impact
Air Force omission of Civil Affairs from the offensive side	CA support to IO: (1) CA encompass activities that military commanders take to establish and maintain relationships between their forces and the civil authorities and general populations, resources, and institutions in friendly, neutral, or hostile areas where their forces are employed. (2) CA activities support the JFC's initiatives to improve relations with friendly foreign military forces and civilian populations and regional strategy and long-term goals by strengthening the capabilities of a host nation in effectively applying its indigenous resources to mitigate or resolve its instability, privation, or unrest. (3) CA and PSYOP are mutually supportive within civil-military operations (CMO).[16]	Air Force doesn't possess any dedicated active duty civil affairs assets; however, there are 248 Air Force Reserve lawyers who exclusively support Army civil affairs missions.	1. Lack of synergy that would result from not coordinating and deconflicting Air Force Reserve CA lawyer activities with other IO initiatives.

Difference	Joint	Air Force	Potential Impact
Air Force omission of INFOSEC from the defensive side	Activities and Technologies Supporting IA. (1) INFOSEC is the protection and defense of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. INFOSEC includes those measures necessary to detect, document, and counter such threats. (2) INFOSEC is composed of computer security (COMPUSEC) and COMSEC[17].	Information assurance includes the protection of information systems against unauthorized access or information corruption. It encompasses computer security, communications security, and those measures necessary to detect, document, and counter such threats.[18]	1. Air Force omission of protection and defense against denial of service to authorized users from IA could leave information and information systems vulnerable to these attacks. 2. Lack of synergy that would result from not coordinating and deconflicting Air Force INFOSEC with other IO initiatives.
Air Force omission of PHYSEC from the defensive side	1. Personnel security, industrial security, and physical security measures are examples of procedures contributing indirectly to IA.[19] 2. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC materials and information.[20]	1. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC materials and information.[21]	1. Air Force omission of PHYSEC from IA could leave information and information systems vulnerable to physical attacks. 2. Lack of synergy that would result from not coordinating and deconflicting Air Force PHYSEC with other IO initiatives.

Difference	Joint	Air Force	Potential Impact
Air Force omission of Education, Training & Awareness from the defensive side	A key element of information environment protection is education and training of joint force systems users, administrators, and managers. Awareness heightens threat appreciation and the importance of adhering to joint force protective measures. Education provides the concepts and knowledge to develop appropriate policies, procedures, and operations to protect joint force information systems. Training develops the skills and abilities required to operate while mitigating joint force vulnerabilities.[22]	No doctrinal explanation for omission.	1. Lack of synergy that would result from not coordinating and deconflicting Air Force Education, Training & Awareness with other IO initiatives.
Air Force omission of Intel Support from the defensive side	A critical component of intelligence support is identifying the IO threat. Threat information is a primary input to risk management and directly contributes to information environment protection.[23]	Intelligence analysts strive to accurately estimate an adversary's probable courses of action, including their capability and intentions to conduct IW.[24]	1. Negligible impact since the joint world and Air Force recognize the importance of intelligence to identify the IO/IW threat.

Difference	Joint	Air Force	Potential Impact
Air Force omission of PA from the defensive side	PA programs contribute to information assurance by disseminating factual information. Factual information dissemination counters adversary deception and propaganda.[25]	Air Force commanders must consider how Public Affairs, Combat Camera capabilities, and military information dissemination can convey accurate information to the targeted audiences and mitigate the intended effects of an adversary's psychological operations.[26]	1. Lack of synergy that would result from not coordinating and deconflicting Air Force PA with other IO initiatives.
Air Force omission of Command Information from the defensive side	Command information programs serve the same purpose as PA with respect to defensive IO. Command information programs normally are found within joint force components and at the lower level units where there is no designated PA program.[27]	Air Force commanders must consider how Public Affairs, Combat Camera capabilities, and military information dissemination can convey accurate information to the targeted audiences and mitigate the intended effects of an adversary's psychological operations.[28]	1. Lack of synergy that would result from not coordinating and deconflicting Command Information with other IO initiatives.

Difference	Joint	Air Force	Potential Impact
Air Force omission of Offensive IO support from the defensive side	Offensive IO can be conducted to support defensive IO throughout the range of military operations. Offensive IO must be integrated with defensive IO to provide timely response against identified and potential threats to friendly information and information systems.[29]	Various defensive capabilities are mutually supporting (that is any one can be used as a countermeasure in support of another) and can support offensive activities...However, they can also conflict with each other and with offensive activities if they are used without knowledgeable coordination and integration.[30]	1. Negligible impact since the joint world and Air Force recognize that offensive and defensive activities must be coordinated and integrated.
Air Force use of one of three electronic warfare subdivisions, "electronic protection," on the defensive side rather than the all inclusive term "electronic warfare."	Electronic attack (EA), electronic protection (EP), and electronic warfare support (ES) are examples of EW capabilities contributing to protection and defense of information and information systems.[31]	Electronic protection guarantees the use of the electronic spectrum for friendly forces. Electronic protection is an important part of the defensive DCI mix and must be fully coordinated and integrated with OCI capabilities, activities, and operations.[32]	1. Negligible impact since the Air Force recognizes that offensive and defensive activities must be coordinated and integrated.

Difference	Joint	Air Force	Potential Impact
Air Force use of the term "counterPSYOP" instead of the joint term "counterpropaganda."	Counterpropaganda counters "Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly."[33]	CounterPSYOP counters "Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals."[34] "PSYOP techniques are used to plan and execute truth projection activities intended to inform foreign groups and populations persuasively."[35]	1. Since PSYOP executes truth projection, and propaganda can be "any form of communication" (including falsehoods), it would appear the Air Force is saying that they will counter adversary truths rather than adversary propaganda, which would include both truths and falsehoods. Whether this was the intention of the Air Force is not known.

Notes

[1] Joint Warfighting Center. *Concept for Future Joint Operations: Expanding Joint Vision 2010*, May 1997, 39 and Joint Pub (JP) 3-13, *Joint Doctrine for Information Operations*, 9 October 1998, II-1.
[2] Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, 5 August 1998, 41.
[3] Concept for Future Joint Operations: Expanding Joint Vision 2010, 39.
[4] AFDD 2-5, 2.
[5] JP 3-13, I-9.
[6] AFDD 2-5, 41.
[7] JP 3-13, GL-7.
[8] AFDD 2-5, 42.
[9] Ibid., 40.
[10] JP-3-13, GL-7.
[11] AFDD 2-5, 16.
[12] JP 3-13, II-3.
[13] Ibid., GL-5.
[14] AFDD 2-5, 41.
[15] JP 3-13, II-6.
[16] Ibid., II-6.
[17] Ibid., III-9.
[18] AFDD 2-5, 17.
[19] JP 3-13, III-9.
[20] Ibid., III-9.
[21] AFDD 2-5, 17.
[22] JP 3-13, III-5.
[23] Ibid., III-5.
[24] AFDD 2-5, 22.
[25] JP 3-13, III-7.
[26] AFDD 2-5, 18.
[27] JP 3-13, III-7.

Notes

[28] AFDD 2-5, 18.
[29] JP 3-13, III-7.
[30] AFDD 2-5, 16.
[31] JP 3-13, III-5.
[32] AFDD 2-5, 19.
[33] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 23 March 1994 as amended through 6 April 1999, 356.
[34] Ibid., 358.
[35] JP 3-53, *Doctrine for Joint Psychological Operations*, 10 July 1996, I-5.

Bibliography

Air Force Doctrine Document (AFDD) 1. *Air Force Basic Doctrine*, September 1997.

AFDD 2-5. *Information Operations*, 5 August 1998.

AFDD 2-5 (DRAFT). *Information Operations*, September 2000.

Air University. *Response to "The Air War Over Serbia" Initial Report*. Maxwell AFB, Alabama, May 2000. In United States. Air Command and Staff College. *Joint Forces and Capabilities*. Maxwell AFB, Alabama, January 2001, 243.

Chairman of the Joint Chiefs of Staff. *Joint Vision 2010*, July 1996.

Davis, Lt Col Harry J. "Developing Air Force Information Warfare Operational Doctrine: The Crawl-Walk-Run Approach." Research Report. Maxwell AFB, Alabama: Air War College, 1 April 1996.

Department of the Air Force. *The Air War Over Serbia, Aeropace Power in Operation Allied Force*. Washington, D.C., April 2000, 5.

Englin, 2d Lt David L. *The Lightening Bolt and the Quill: Determining the Role of Air Force Public Affairs in Information Warfare*. Masters diss., Harvard University, 1998.

Henning, Maj Paul R. "Air Force Information Warfare Doctrine: Valuable or Valueless? Research Report no. 97-0604C. Maxwell AFB, Alabama: Air Command and Staff College, March 1997.

Hollman, Capt Ryan D. *A Descriptive Study of Information Operations and Information Warfare Awareness in the United States Air Force*. Masters diss., Air Force Institute of Technology, September 1998.

Hubbard, LTC Zachary P. "Information Warfare in Kosovo." *Journal of Electronic Defense*, (November 1999): 58.

Joint Pub (JP) 0-2, *Unified Action Armed Forces (UNAAF)*, 24 February 1995.

JP 1. *Joint Warfare of the Armed Forces of the United States*, 10 January 1995.

JP 1-01. *Joint Doctrine Development System*, 5 July 2000.

JP 1-01.1. *Compendium of Joint Publications*, 23 April 1999.

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 23 March 1994 as amended through 6 April 1999.

JP 3-13. *Joint Doctrine for Information Operations*, 9 October 1998.

JP 3-53, *Doctrine for Joint Psychological Operations*, 10 July 1996.

JP 3-61, *Doctrine for Public Affairs in Joint Operations*, 14 May 1997.

Joint Warfighting Center. *Concept for Future Joint Operations: expanding Joint Vision 2010*, May 1997.

Newell, Maj Mark R. "Tactical-Level Public Affairs and Information Operations." *Military Review*, no. 6 (December 1998-February 1999): 22.

Pounder, Maj Gary. "Opportunity Lost: Public Affairs, Information Operations, and the Air War Against Serbia." *Airpower Journal*, Volume XIV, No. 2 (Summer 2000).